IN THE UNITED STATES DISTRICT COURT
FOR EASTERN DISTRICT OF PENNSYLVANIA

IN THE MATTER OF THE SEARCH OF: 574 E. CHESTNUT STREET, APT. 1, COATESVILLE, PENNSYLVANIA 19320 IN THE MATTER OF: THE COMPLAINT AGAINST BIANCHA KRANZLEY	Case Nos. 20-MJ-1622, 1623

AFFIDAVIT IN SUPPORT OF AN APPLICATION UNDER RULE 41 FOR A WARRANT TO SEARCH AND SEIZE AND FOR A COMPLAINT

I, Nicholas Leonard, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of:

   a. a criminal complaint charging Biancha Kranzley with fraud in connection with major disaster or emergency benefits, in violation of 18 U.S.C. § 1040; and

   b. an application under Rule 41 of the Federal Rules of Criminal Procedure for a warrant to search the premises known as 574 E. Chestnut Street, Apt. 1, Coatesville, Pennsylvania 19320, hereinafter "Premises," further described in Attachment A, for the things described in Attachment B.

2. I am a Special Agent with the Federal Bureau of Investigation and am a Certified Fraud Examiner (CFE). I am currently assigned to the Financial Institution Fraud squad. As part of my duties as a Special Agent, I investigate violations and alleged violations of federal laws, including but not limited to violations of 18 U.S.C. § 1040. I have been trained in various aspects of law enforcement, including the investigation of financial offenses. Through my

education and experience and that of other agents, I have become familiar with the methods that individuals use in furtherance of committing the various offenses involved in these financial fraud schemes. I have participated in investigations that have resulted in the arrest of individuals who have committed various financial fraud crimes as well as the seizure of evidence in support of these crimes. Through my training and experience, I am familiar with digital evidence commonly possessed and used by those involved in criminal activities in all forms of media.

3. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested complaint and warrant, and search warrant, and does not set forth all of my knowledge about this matter.

BACKGROUND

4. On March 13, 2020, the President declared the ongoing COVID-19 pandemic to be an emergency under Section 501(b) of the Robert T. Stafford Disaster Relief and Emergency Assistance Act.

5. On March 27, 2020, the Coronavirus Aid, Relief, and Economic Security Act ("CARES Act") was signed into law. The CARES Act created the Pandemic Unemployment Assistance ("PUA") program, which provides unemployment benefits, including unemployment

insurance ("UI"), to individuals not eligible for regular unemployment compensation or extended unemployment benefits.

6. The PUA program is administered by the various states, including the Commonwealth of Pennsylvania, but its benefits are funded in part by the federal government. In Pennsylvania, the Pennsylvania Department of Labor and Industry ("PA DLI") administers the PUA program.

7. Individuals are only eligible for PUA benefits if they are unemployed for reasons related to the COVID-19 pandemic and are available to work. In order to receive benefits, an individual must file a claim including his or her name, social security number, and address, as well as, answer the eligibility questions.

8. To be eligible to request weekly PUA benefits, applicants must certify, under penalty of perjury, that they are available for work and if offered a job, are able to report to that job on the day it is offered. Earnings must be reported for each week a person works and applicants must read and understand the PUA Compensation Handbook.

9. To combat fraud in the PUA program, beginning in June of 2020, PUA benefits were issued via prepaid US Bank Visa debit cards and mailed to the residential addresses on the PUA applications.

FRAUD IN CONNECTION WITH MAJOR DISASTER OR EMERGENCY BENEFITS

10. 18 U.S.C. § 1040 provides:

(a) Whoever, in a circumstance described in subsection (b) of this section, knowingly—

(1) falsifies, conceals, or covers up by any trick, scheme, or device any material fact; or

(2) makes any materially false, fictitious, or fraudulent statement or representation, or makes or uses any false writing or document knowing the same to contain any materially false, fictitious, or fraudulent statement or representation,

in any matter involving any benefit authorized, transported, transmitted, transferred, disbursed, or paid in connection with a major disaster declaration under section 401 of the Robert T. Stafford Disaster Relief and Emergency Assistance Act (42 U.S.C. 5170) or an emergency declaration under section 501 of the Robert T. Stafford Disaster Relief and Emergency Assistance Act (42 U.S.C. 5191), or in connection with any procurement of property or services related to any emergency or major disaster declaration as a prime contractor with the United States or as a subcontractor or supplier on a contract in which there is a prime contract with the United States, shall be fined under this title, imprisoned not more than 30 years, or both.

(b) A circumstance described in this subsection is any instance where--

(1) the authorization, transportation, transmission, transfer, disbursement, or payment of the benefit is in or affects interstate or foreign commerce;

(2) the benefit is transported in the mail at any point in the authorization, transportation, transmission, transfer, disbursement, or payment of that benefit; or

(3) the benefit is a record, voucher, payment, money, or thing of value of the United States, or of any department or agency thereof.

(c) In this section, the term "benefit" means any record, voucher, payment, money or thing of value, good, service, right, or privilege provided by the United States, a State or local government, or other entity.

SUMMARY OF INVESTIGATION

11. I am investigating a scheme to defraud the PUA program. Based on the evidence set forth below, there is probable cause to believe that Kranzley has engaged in a scheme to defraud the Pennsylvania PUA.

12. Specifically, based on my investigation to date, Kranzley has perpetrated a scheme to file a PUA application of behalf of her boyfriend, Person 1, who, at the time the application was filed, was incarcerated at the Chester County Prison ("CCP"), in West Chester, Pennsylvania. The PUA application falsely represented that Person 1 was available to work, and that he had lost his job due to the COVID-19 pandemic. In fact, Person 1 has been incarcerated at CCP since at least mid-2019, and at the time of the filing of the application, was not able to work. As a result of the fraudulent application, the Commonwealth of Pennsylvania has paid out more than $13,000 in unauthorized PUA payments.

13. Based on the information contained herein, there is probable cause to believe that Kranzley has violated 18 U.S.C. § 1040. Further, for the reasons described below, there is probable cause to believe that evidence of the crimes will be found at the Premises.

PROBABLE CAUSE

The PUA Application

14. On or about July 4, 2020, a claim for PUA benefits was submitted on behalf of Person 1.

15. According to records collected from PA DOL, Person 1's PUA claim was submitted from IP address 108.16.111.251. According to records collected from Verizon, that IP address on July 4, 2020, was assigned to Kranzley at the Premises. The Verizon internet service was originally assigned to Kranzley on May 22, 2019, and remained assigned to Kranzley as of September 2020, when Verizon supplied the information.

16. Based on those Verizon records, there is probable cause to believe that the Premises contains a router that used the IP address 108.16.111.251, and computer equipment that connects both wirelessly and physically to the router. Based on my training and experience, and as explained below, there is probable cause to believe that the router and computer equipment contain evidence of the crimes under investigation, including evidence that the computer equipment was used to access, prepare, and submit the PUA application.

17. Person 1's PUA application lists the "User Name" of the person who submitted it as "BCKRANZ." The application also lists the email address of the person who submitted it as Bianchakranzley@gmail.com. Finally, the application lists the mailing address of the application as the Premises.

18. There is probable cause to believe that Kranzley lives at the Premises. First, during a September 16, 2020, interview of Kranzley, which is described in more detail below, the law enforcement agents who conducted the interview found her inside the Premises. Second, her Pennsylvania driver's license, which I have reviewed, lists the Premises as her address. Third, as noted above, Verizon records show that Kranzley subscribes to internet service at the Premises. Fourth, Verizon Wireless records show that Kranzley subscribes to a mobile phone bearing the telephone number 610-350-8262, and that her address is the Premises. Finally, review of a law enforcement database indicates that Kranzley lives at the Premises.

19. There is probable cause to believe that the email account bianchakranzley@gmail.com (the "email account") belongs to Kranzley. According to subscriber records provided by Google, the owner of the email account is "Biancha Kranzley" and the "recovery SMS" is 610-350-8262" which, according Verizon Wireless records, is a mobile phone number assigned to Kranzley. Additionally, according to Google records that were collected by Google on or about August 18, 2020, the last login to the email account occurred on August 5, 2020 from the IP address 108.16.111.251, which according to Verizon records, belongs to Kranzley.

20. Based on my training and experience, the address and the email address, in conjunction with the IP address, and the recorded telephone calls described below, establish probable cause to believe that Kranzley filed the PUA application on behalf of Person 1 from the Premises.

21. According to the docket sheet in the matter of Commonwealth of Pennsylvania v. Person 1, which caused Person No. 1 to be incarcerated at CCP, at the time the claim was submitted, Person 1 was a prisoner at CCP, where he was being held pending trial on a variety of charges. According to the docket sheet, he has been a prisoner since on or about January 2, 2019. Although the docket sheet shows that he posted bail on or about March 21, 2019, records reflect that his bail was revoked on or about May 3, 2019. According to the docket sheet, Person 1 has been in custody since that date.

22. Person 1's PUA claim contained several representations which there is probable cause to believe were false.

23. In response to the question "If offered a job, are you able and available to accept it?[,]" Person 1's application answered "Yes." Given that Person 1 was in custody at the time the application was submitted, there is probable cause to believe that answer was false.

24. In response to the question "Are you unemployed as a direct result of a pandemic or major disaster?[,]" Person 1's application answered "Yes." There is probable cause to believe that the COVID-19 pandemic, which occurred more than one year after Person 1 had initially been incarcerated, played no role in his unemployment.

25. In response to the statement "[t]o be eligible for benefits each week you MUST be able to go to work each day. If you were offered a job today, you must be able to accept it[,]" Person 1's application answered "Yes." Given that Person 1 was incarcerated at the time the PUA application was submitted, there is probable cause to believe that the answer was false.

The Weekly Certifications

26. According to my discussions with a special agent employed by the United States Department of Labor, I know that an applicant must not only submit an application but must also submit weekly certifications, in order to receive PUA funds.

27. The weekly certifications which were filed on behalf of Person 1 also contained false representations.

28. In response to the question "How did the COVID-19 pandemic cause your unemployment?" Person 1's weekly certifications included the answer "You are an independent contractor/gig worker who has been forced to significantly limit his or her performance of customary work activities because of the COVID-19 public health emergency and are experiencing a diminution of work." There is probable cause to believe that this answer was false because Person 1 was not an independent contractor or gig worker whose hours had been limited by COVID-19 but instead was a prisoner at the Chester County Prison.

29. Moreover, Person 1's weekly certification answered "Yes" to the question "Other than for reasons that were the direct result of the disaster/pandemic, were you able and available to go to work during the week?" There is probable cause to believe that this answer was false. Person 1 was not available to go to work during the week because he was incarcerated.

30. My review of the records showing the submission of Person 1's weekly certifications shows that on July 16, 2020, there were 20 certifications submitted for the weeks between February 23, 2020, and July 5, 2020. My review of the submission records shows that

all 20 certifications were filed from the same IP address. Although records collected from Verizon show that the user of the IP address is not ascertainable, there is probable cause to believe that Person 1's sister was responsible for some of these filings. During a recorded telephone call between Kranzley and Person 1 on July 16, 2020, Kranzley told Person 1 that Person 1's sister sent Kranzley pictures of the "PUA thing." Kranzley went on to explain that Person 1's sister "filed weekly." There is probable cause to believe that Kranzley was telling Person 1 that Person 1's sister filed some if not all of the 20 weekly certifications.

31. In addition, the submission records show that the weekly certification for the week of July 26, 2020, was filed on August 6, 2020, from the IP address 108.16.111.251, which, as described above, belongs to Kranzley. During a recorded telephone call that day, Kranzley told Person 1 that she "did your PUA thing again." There is probable cause to believe that she was informing Person 1 that she had submitted the PUA weekly certification on his behalf. That certification contained the misrepresentations described above.

Bank Records

32. Based on records collected from US Bank, Person 1 received $13,555 for his PUA claim between on or about July 20, 2020, and on or about July 31, 2020. The mailing address listed on the bank statement was the Premises. Based on my training and experience, there is probable cause to believe that statements and other bank records relating to this account will be found at the Premises. Based on information provided by US Bank, there is also probable cause to believe that the debit card associated with that account would have been mailed to the

Premises. Because Person 1 is incarcerated, there is probable cause to believe that Kranzley would have kept custody of the debit card.

33. Records from US Bank also show that the US Bank account containing the funds from Person 1's PUA application was accessed twelve times on July 28 and 29, 2020. Eleven of those instances occurred from IP address 108.16.111.251, which, as noted above, is assigned to Kranzley at the Premises. The twelfth occurred from an IP address which, based on my review of open source records, is assigned to AT&T cellular network.

34. The US Bank records also show purchases made with the debit card associated with the account. There is probable cause to believe that a purchase made on July 30, 2020 for $167.79 at a Wal-Mart in Parkesburg, Pennsylvania, is attributable to Kranzley. Per records from Wal-Mart, I have collected the receipt from that transaction, which shows, in the "Guest Info" section, Kranzley's name. I have also collected and reviewed photographs of the person who conducted the transaction. My colleague, who interviewed Kranzley on September 16, 2020, confirmed that the photograph shows Kranzley.

The Telephone Calls

35. Person 1 engaged in a number of telephone calls, which were recorded by CCP, in which he discussed his PUA application, as well as what there is probable cause to believe was an application for normal unemployment benefits. Many of those calls included Kranzley.

36. During a series of telephone calls on July 1, 2020, between Person 1 and Kranzley, using the telephone number 610-350-8262, which she confirmed was her number, the

two discussed filing an unemployment application on Person 1's behalf. At the end of the discussion, Kranzley told Person 1 "I submitted it."

37. During a telephone call the next day, Person 1 told Kranzley that the application she had filed the previous day, which he referred to using the colloquialism "jawn," "is not the only jawn you can file." Person 1 instructed Kranzley to search the internet for "PUA." Kranzley responded "I see it now—Pennsylvania Pandemic Unemployment Insurance." Based on this conversation, there is probable cause to believe that Kranzley first filed an application on Person 1's behalf for ordinary unemployment benefits.

38. Person 1 asked Kranzley to file a PUA application on his behalf. After some discussion, Kranzley agreed: "Alright, I'll have to do that tonight then." Person 1 told Kranzley to "take the twenty-five, take whatever you need." There is probable cause to believe that Person 1 was telling Kranzley to take a portion of the fraudulent PUA funds for herself.

39. In a July 3, 2020, telephone call, Person 1 asked Kranzley if she had submitted the application. She said that she had started it, but had not finished it. She claimed that she intended to finish it later that day, perhaps using a computer at her work site.

40. In a subsequent call on July 3, 2020, Person 1 asked again whether she had completed the application. This time, Kranzley confirmed that she had completed the application.

41. In a July 14, 2020, telephone call with Kranzley at 610-350-8262, Kranzley told Person 1 "I got two pieces of mail for you and one of them says . . . it was denied." She went on to explain:

> So when I go online, it doesn't say denied. So I'm thinking like one of them, you know, was going to have the debit card in it or whatever. Um, but it said, because there was no record of wages for the year, that's why. Like but, you can file for an appeal.

42. When Kranzley told Person 1 that she did not understand the letter, Person 1 responded "I don't know, but mothafuckers that are getting it, I mean, like, I was an entrepreneur before–you I'm saying." To which Kranzley responded:

> And I put that in there, like, you know, you were, um,self-employed, um, I put like, the business name, um, and then like stuff that it was asking as far as like the wages and stuff, like how to prove—it was like, do you keep receipts from, you know, work, or do you have any kind of documentation. That's the only kind of thing that [UI]

43. Based on my review of the telephone recordings, there is probable cause to believe that the denial letter received by Kranzley related to the claim Kranzley filed on Person 1's behalf for normal unemployment benefits. In any event, based on my review of PA DLI records, it is clear that Person 1's PUA application was filed and that the Commonwealth of Pennsylvania has made payments pursuant to that application.

44. In a telephone call on July 28, 2020, Kranzley and Person 1 discussed what to do with the money. Person 1 suggested to Kranzley that she remove the money from the debit card account. Kranzley responded that she was going to do that anyway—"I'm not keeping it on the card. We ain't stupid out here." Based on my training and experience, there is probable cause to

believe that Kranzley and Person 1 had agreed to remove the money from the card to limit the government's ability to recoup the funds later if the fraud were discovered. The US Bank records show one or more ATM withdrawals of $800 on August 2, 3, 6, 11, 16. The ending balance on the account as of September 10, 2020 was $5,726.12, from the original $13,555.

45. Based on the nature of the recorded discussion between Kranzley and Person 1, there is probable cause to believe that Person 1 caused Kranzley to submit the PUA application, which contained false statements. Given that the recorded warning at the beginning of each inmate telephone call informed Kranzley that Person 1 was incarcerated, there is probable cause to believe that Kranzley would have known that Person 1's PUA application contained the false representations described above.

46. Given that Kranzley used her mobile phone to communicate with Person 1 about the PUA application, there is probable cause to believe that the mobile phone contains evidence of the crimes under investigation, including records of incoming and outgoing calls with Person 1, Person 1's sister, and others, as well as voicemails, text messages, and other forms of communication.

The Interview

47. On or about September 16, 2020, investigators conducted a partial interview of Kranzley. The interview occurred at the Premises, where Kranzley admitted to living. On that day, Agents knocked and announced at the front door of the Premises, but received no answer. They then proceeded around the right side of the house (from the perspective of E. Chestnut

Street) and found a side door, which was light in color. When they knocked and announced at the side door, which is indicated in Attachment A with arrows, Agents observed Kranzley open the side door from inside. That side door is the entrance that agents will use to execute the search warrant.

48. Kranzley admitted that 610-350-8262 is her telephone number. Kranzley told investigators that she and Person 1 were in a romantic relationship. She also confirmed that she knew that Person 1 had been incarcerated for 20 months.

49. When investigators asked Kranzley about her role in preparing and filing the false PUA application, she told them that she had set up an account for Person 1 to file the application but denied having prepared or filed the application. Instead, she claimed that she had provided the login information to Person 1's sister and that Person 1's sister had prepared and filed the PUA application. Kranzley showed investigators a text message on her mobile phone between Kranzley and who she claimed was Person 1's sister. The text message, which investigators did not review in its entirety at that point, included the login name and password for the PUA application. There is probable cause that Kranzley's mobile phone contains text messages and other communications with Person 1's sister and others, relating to the fraud scheme under investigation. However, in light of the telephone recordings and IP address information described above, there is probable cause to believe that Kranzley's statement that she did not file the application was false.

50. Near the end of the interview, Kranzley also mentioned to investigators that Person 1 had had a prison job, implying that such a job might support a claim for PUA benefits. According to CCP records that I have reviewed, Person 1 was employed in the prison laundry facility until April 2020, at which point laundry service was outsourced because one of the laundry employees tested positive for COVID-19. According to the Pennsylvania Office of Unemployment Compensation's website (https://www.uc.pa.gov/unemployment-benefits/file/Pages/Filing-for-PUA.aspx (last visited October 1, 2020)), this prison job does not, as a legal matter, support the PUA claim. Nor did Kranzley believe that, in submitting the fraudulent application for benefits, Person 1's prison job supported the PUA claim. First, in the recorded discussions that I reviewed, there was no mention of basing the PUA claim on Person 1's prison job. Second, in the section of the application that asked for Person 1's net earnings during the four quarters of 2019, Kranzley answered $0; if she had meant to base the claim on Person 1's prison job, she would have listed the funds he had earned doing that job. Third, in answering the question "[w]hat is the date that you last performed work?," Kranzley answered December 31, 2018—the day before Person 1 was arrested. Finally, in submitting the weekly certification for the week of July 26, 2020 through August 1, 2020, Kranzley asserted that Person 1 was "an independent contractor/gig worker who has been forced to significantly limit his or her performance of customary work activities because of the COVID-19 public health emergency and are experiencing a diminution of work." This description is flatly inconsistent with the Person 1's prison job.

51. Kranzley ended the interview quickly, claiming that she had to pick up her children in Morgantown, Pennsylvania. She agreed to return to the Premises after picking up her children in order to conclude the interview. Investigators waited for two hours but Kranzley never returned.

52. While investigators were waiting for Kranzley to return, they observed another woman enter the Premises. Upon her exit, they questioned her briefly. She identified herself as Person 1's mother and she told investigators that Kranzley had called her to say that investigators had questioned her. There is probable cause to believe that Kranzley, after the interview concluded, had communicated with others about the interview. Based on my training and experience, there is probable cause to believe that Kranzley's mobile phone would contain evidence of discussions she had with others about the interview and about her role in the conduct under investigation.

TECHNICAL TERMS

53. Based on my training and experience, I use the following technical terms to convey the following meanings:

a. IP Address: The Internet Protocol address (or simply "IP address") is a unique numeric address used by computers on the Internet. An IP address looks like a series of four numbers, each in the range 0-255, separated by periods (e.g., 108.16.111.251). Every computer attached to the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer may be

directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.

b. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

c. Storage medium: A storage medium is any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

COMPUTERS, ELECTRONIC STORAGE, AND FORENSIC ANALYSIS

54. As described above and in Attachment B, this application seeks permission to search for records that might be found on the Premises, in whatever form they are found. One form in which the records might be found is data stored on a computer's hard drive or other storage media. Thus, the warrant applied for would authorize the seizure of electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

55. *Probable cause.* I submit that if a computer or storage medium is found on the PREMISES, there is probable cause to believe those records will be stored on that computer or storage medium, for at least the following reasons:

a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

c. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system

configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

56. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how computers were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any storage medium in the Premises because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and

passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.

b. As explained herein, information stored within a computer and other electronic storage media may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a computer or storage media (e.g., registry information, communications, images and movies, transactional information, records of session times and durations, internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculpating or exculpating the computer owner. Further, computer and storage media activity

can indicate how and when the computer or storage media was accessed or used. For example, as described herein, computers typically contain information that log: computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (e.g., a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculpate or exculpate the computer user. Last, information stored within a computer may provide relevant insight into the computer user's state of mind as it relates to the offense under investigation. For example, information within the computer may indicate the

owner's motive and intent to commit a crime (e.g., internet searches indicating criminal planning), or consciousness of guilt (e.g., running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

c. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence

of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

f. I know that when an individual uses a computer to file a false PUA application, the individual's computer will generally serve both as an instrumentality for committing the crime, and also as a storage medium for evidence of the crime. The computer is an instrumentality of the crime because it is used as a means of committing the criminal offense. The computer is also likely to be a storage medium for evidence of crime. From my training and experience, I believe that a computer used to commit a crime of this type may contain: data that is evidence of how the computer was used; data that was sent or received; notes as to how the criminal conduct was achieved; records of Internet discussions about the crime; and other records that indicate the nature of the offense.

57. *Necessity of seizing or copying entire computers or storage media.* In most cases, a thorough search of a premises for information that might be stored on storage media often requires the seizure of the physical storage media and later off-site review consistent with the warrant. In lieu of removing storage media from the premises, it is sometimes possible to make an image copy of storage media. Generally speaking, imaging is the taking of a complete electronic picture of the computer's data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded

on the storage media, and to prevent the loss of the data either from accidental or intentional destruction. This is true because of the following:

a. The time required for an examination. As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a computer has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable. As explained above, because the warrant calls for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine storage media to obtain evidence. Storage media can store a large volume of information. Reviewing that information for things described in the warrant can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.

b. Technical requirements. Computers can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on the Premises. However, taking the storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.

c. Variety of forms of electronic media. Records sought under this warrant could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.

58. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit seizing, imaging, or otherwise copying storage media that reasonably appear to contain some or all of the evidence described in the warrant, and would authorize a later review of the media or information consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

59. Because several people share the Premises as a residence, it is possible that the Premises will contain storage media that are predominantly used, and perhaps owned, by persons who are not suspected of a crime. If it is nonetheless determined that that it is possible that the things described in this warrant could be found on any of those computers or storage media, the warrant applied for would permit the seizure and review of those items as well.

60. Additionally, based on my training and experience, there is probable cause to believe that internet service equipment, including any router, will contain evidence of which devices accessed the internet from the Premises. There is probable cause to believe that such internet service equipment contains evidence of the crimes under investigation.

CONCLUSION

61. I submit that this affidavit sets forth probable cause for:

a. a criminal complaint charging Biancha Kranzley with fraud in connection with major disaster or emergency benefits, in violation of 18 U.S.C. § 1040; and

b. a warrant to search the Premises described in Attachment A and seize the items described in Attachment B.

REQUEST FOR SEALING

62. It is respectfully requested that this Court issue an order sealing, until further order of the Court, all papers submitted in support of this application, including the application and search warrant. I believe that sealing this document is necessary because the items and information to be seized are relevant to an ongoing investigation into the criminal organizations as not all of the targets of this investigation will be searched at this time. Based upon my training and experience, I have learned that online criminals actively search for criminal affidavits and search warrants via the Internet, and disseminate them to other online criminals as they deem appropriate, i.e., post them publicly online through the carding forums. Premature disclosure of the contents of this affidavit and related documents may have a significant and negative impact on the continuing investigation and may severely jeopardize its effectiveness.

Respectfully Submitted,

/s/ Nicholas Leonard
NICHOLAS LEONARD
SPECIAL AGENT
FBI

Subscribed and sworn to before me
On October 1, 2020:

HON. HENRY S. PERKIN
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

Property to be searched

The property to be searched is 574 E. Chestnut Street, Apt. 1, Coatesville, PA, 19320, further described as a reddish brown brick house with brown siding and a grey door, which is approximately five steps above the street. The entrance to Apartment 1, is on the right side of the building (when viewed from the street). The red arrows in the second and third photographs indicate the location of the light-colored door that Kranzley answered when agents interviewed her on September 16, 2020. That is the door that agents will use to execute the search warrant.


E Chestnut St
E Chestnut St
E Chestnut St
E Chestnut St
E Chestnut St
E Chestnut St
574 East Chestnut Street
E Diamond St
E Diamond St
E Diamond St
E Diamond St

ATTACHMENT B

Property to be seized

1. All records relating to violations of 18 U.S.C. § 1040 (major disaster fraud), those violations involving Person 1, Person 1's sister, and Biancha Kranzley, and occurring after July 1, 2020, including:

   a. Bank records relating to any US Bank account in the name of Person 1;

   b. Records relating to a mobile telephone bearing the telephone number 610-350-8262;

   c. Communications between Biancha Kranzley and Person 1;

   d. Communications between Biancha Kranzley and Person 1's sister;

   e. Communications pertaining to the submission of PUA applications;

   f. Records and information relating to efforts to defraud the PUA program;

   g. Records and information relating to the preparation, submission, or review of any PUA application;

   h. Records and information relating to the receipt or use of any funds from the PUA program;

   i. Records and information relating to the e-mail account bianchakranzley@gmail.com;

   j. Records and information relating to the identity or location of those involved in the scheme under investigation;

2. Computers, mobile phones, electronic devices, or storage media used as a means to commit the violations described above, including by submitting the false PUA application.

3. For any computer, mobile phone, electronic devices, or storage medium whose seizure is otherwise authorized by this warrant, and any computer, mobile phone, electronic devices or storage medium that contains or in which is stored records or information that is otherwise called for by this warrant (hereinafter, "COMPUTER"):

a. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;

b. evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

c. evidence of the lack of such malicious software;

d. evidence indicating how and when the computer was accessed or used to determine the chronological context of computer access, use, and events relating to crime under investigation and to the computer user;

e. evidence indicating the computer user's state of mind as it relates to the crime under investigation;

f. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;

g. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the COMPUTER;

h. evidence of the times the COMPUTER was used;

i. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;

j. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;

k. records of or information about Internet Protocol addresses used by the COMPUTER;

l. records of or information about the COMPUTER's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses;

m. contextual information necessary to understand the evidence described in this attachment.

4. Routers, modems, and network equipment used to connect computers to the Internet.

As used above, the terms "records" and "information" includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

The term "computer" includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

The term "storage medium" includes any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

This warrant authorizes a review of electronic storage media and electronically stored information seized or copied pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the seized or copied electronic data to the custody and control of attorneys for the government and their support staff for their independent review.